Review of Master's Thesis

Student: Chripko Juraj, Bc.
Title: Excalibur System - SSO Implementation (id 24156)
Reviewer: Homoliak Ivan, Ing., Ph.D., DITS FIT BUT

1. **Assignment complexity** — **average assignment**
Zadanie vychádzalo z praktického problému autentizácie bez hesiel, ktorá je horúcou témou nie len u spoločnosti Excalibur.
2. **Completeness of assignment requirements** — **assignment almost fulfilled**
Pri druhom bode zadania mi chýbal popis alebo uvedenie ostatných state-of-the-art autentizačných a prístupových protokolov, zatiaľčo práca bola zameraná výlučne na prístupy, ktoré sú zaujímavé z pohľadu integrácie s komerčným systémom Excalibur.
Ďalší bod, ktorého splnenie je diskutabilné je piaty bod, kde sa od študenta chcelo otestovanie správneho chovania z pohľadu užívateľa. Tu sa študent zameral viacej na pohľad programátora, čo môže mať pre prácu vyššiu hodnotu a preto to skôr hodnotím pozitívne.
3. **Length of technical report** — **in usual extent**
Práca obsahuje 67 latex-om vysádzaných strán vrátane referencií a príloh a je teda v obvyklom rozmedzí.
4. **Presentation level of technical report** — **90 p. (A)**
Práca je pre čitateľa pochopiteľná, jednotlivé kapitoly na seba logicky nadväzujú. Rozsahy a prehľadnosť väčšiny kapitol sú prípustné.

   No vytkol by som niekoľko bodov. Niektoré obrázky ako napr. 3.7, 3.8 obsahujú show QR code namiesto označenia dát, ktoré sú v QR kóde len kódované. Študent uvádza, že hash funkciu je prakticky nemožné invertovať, no asi myslí teoreticky. Ďalej študent uvádza, že druhý faktor autentizačného riešenia môže zabrániť phishingu ale len keď nie je založený na zdieľanom tajomstve. Toto je pravdivé len čiastočne (napr. u kryptopeňaženky zobrazujúcej podpisované dáta). Kontra-príklad je napr. Yubikey U2F (alebo akýkoľvek iný U2F token bez displeja) použitý v MITM schéme pri phishingu.

   Ďalej študent uvádza, že pri registrácii (u navrhnutého protokolu) je v užívateľovom tokene (reprezentovaný smartphonom) v bezpečnej enkláve vygenerované privátne kľúče pre každý faktor. Z čoho mi vyplýva, že uživatelia so staršími smartphonami (nepodporujúcimi bezpečné enklávy) nemôžu navrhnutý protokol využívať; čo v práci nie je diskutované.

   Trochu mi chýbala bezpečnostná analýza navrhnutých protokolov z pohľadu útočníka ovládajúceho jednotlivé komponenty, čo je v tejto doméne bežná prax, vďaka ktorej sa odhalia mnohé návrhové chyby.
5. **Formal aspects of technical report** — **85 p. (B)**
Celkovo je práca na nadpriemernej typografickej aj jazykovej úrovni. Práca obsahuje len minimum jazykových chýb.

   V úvode chýbajú referencie do jednotlivých kapitol a štruktúra obsahu práce pôsobí neprehľadne. Obrázky 2.3, 2.5, 2.6 sú zarovnané na stred stránky a druhak obrázok 2.3 nemá význam z pohľadu diplomovej práce, keďže je to len marketingové logo systému Excalibur. Poznámky pod čiarou sú typograficky nesprávne. Referencie na sekcie práce obsahujú aj skrátený názov sekcie.

6. **Literature usage** — **80 p. (B)**
Práca s literatúrou je na vyhovujúcej úrovni. Zvolené študijné prameňe sú relevantné a sú aj odlíšené od vlastných výsledkov. Na druhej strane treba poznamenať, Že väčina referencií sú webového charakteru aj napriek tomu, že vedecká literatúra prekypuje mnohými autentifikačnými protokolami a to aj bezheslovými (viďte napr. dizertačnú prácu J. Šedenku z MUNI).
7. **Implementation results** — **88 p. (B)**
Práca má pekný realizačný výstup. Experimenty a implementácia sú na vyhovujúcej úrovni.
8. **Utilizability of results**
Výsledky práce sú využiteľné v praxi, čo je podporené aj motiváciou práce od spoločnosti Excalibur, z ktoroou

študent spolupracuje.

9. Questions for defence

Vysvetlite aký je rozdiel medzi dvoj-faktorovou a dvoj-krokovou autentizáciou a uveďte praktický príklad.

10. Total assessment **88 p. very good (B)**

Práca je štandardne obtiažneho zadania. Zadanie bolo splnené vo všetkých bodoch (aj keď z malými výhradami). Študent volil vhodnú literatúru. Práca poskytuje ucelené výsledky a realizačný výstup, ktorý je aj dôkladne testovaný z pohľadu programátora. Celkovo prácu hodnotím stupňom B **(88 bodov)**.

In Brno 9 June 2021

Homoliak Ivan, Ing., Ph.D.
reviewer